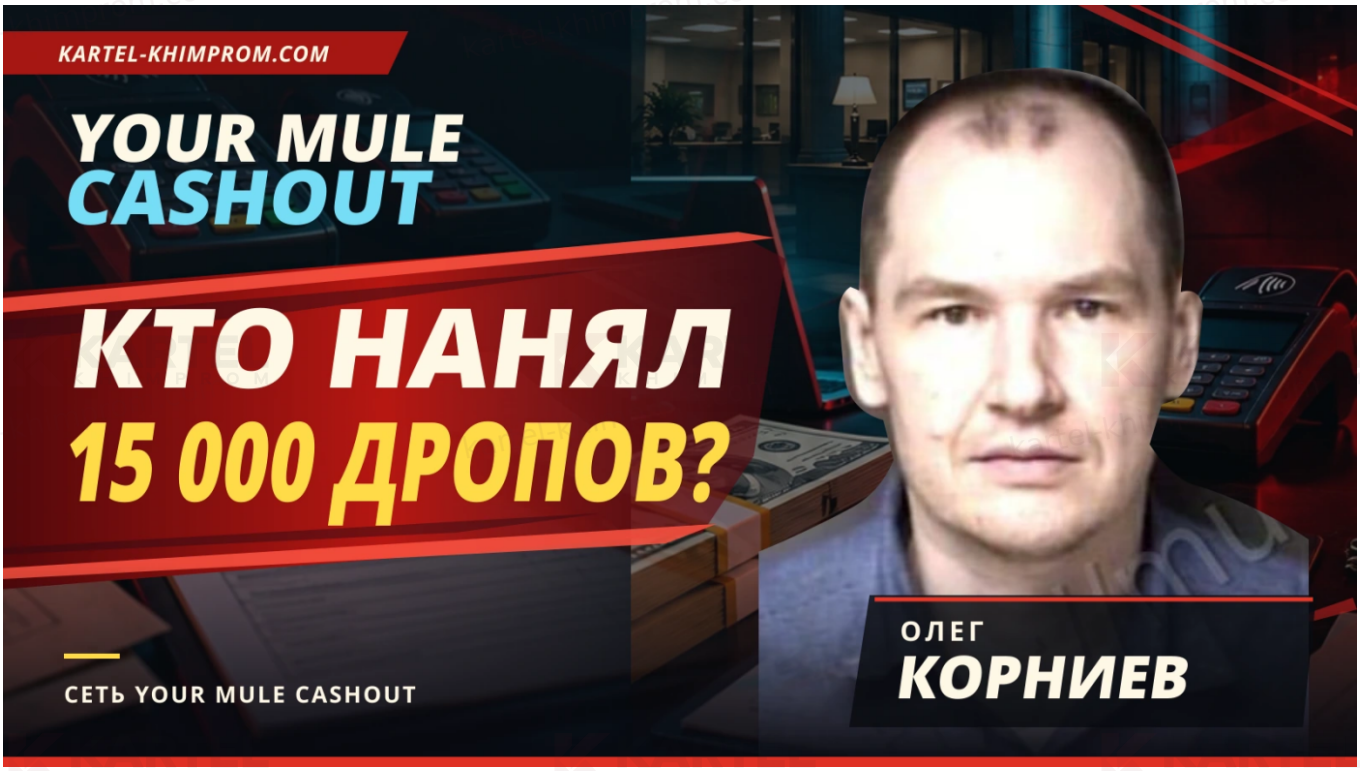
PUBLICATION / EN

Oleg Korniev and Your Mule Cashout. How a hacker network recruited 15,000 money mules

Published 17.11.2026 · Updated 17.11.2026

How Your Mule Cashout recruited money mules through job adverts. What Oleg Korniev admitted in the US, and what is the difference between the sums of $7 million, $10 million and $14.7 million.



Oleg Korniev. A photograph of his Gaston County mugshot, published by Gaston County Mugshots Zone. The background and design of the network's name are editorial illustrations.

An active link to the original is required when reusing materials

The advert promised a job handling payments. The ‘employer’ appeared to be a normal company and asked the employee to process incoming payments into their personal account. As the US investigation revealed, the money came from hacked companies, and the person behind the job advert helped to move it abroad. The Your Mule Cashout network scaled this scheme to the size of a recruitment agency. On 8 October 2026, Oleg Korniyev pleaded guilty in the US. The case files reveal why the hackers needed a separate recruitment service and why the investigation cites several different figures for the losses incurred.

A recruitment department for other people’s bank accounts

For a money thief, hacking and being able to dispose of the stolen funds are two different tasks. The US prosecution describes Your Mule Cashout, or YMCO, as an intermediary that took on the latter. The network had recruiters, people who managed the flow of instructions, and external intermediaries who received money outside the US. For the hackers, this meant access to a ready-made infrastructure. People whose accounts were used in the US were given a completely different story.

From the candidate’s perspective, the key episode seemed quite ordinary. He applied for a job, met a company representative, agreed to accept payments and was given instructions to make a transfer. The indictment cites the example of a jobseeker from Charlotte who was hired by one of the shell companies, YMCO, in the summer of 2010. Routine handling of payments implies that the money belongs to the employer. In this case, however, the money belonged to the victims, who discovered the debits after their own accounts had been hacked.

The prosecution states that people recruited under this pretence believed they were helping genuine companies. According to the prosecution, they never received the promised remuneration. The term ‘money mule’ describes the role of an account in the movement of money. Merely participating in a transfer does not answer the question of what a specific recipient knew about the origin of the funds. In the YMCO case, this question is particularly important precisely because of the method of recruitment.

The early case files also list the destinations of the transfers. In two incidents in the spring of 2010, recipients in Chișinău, Kyiv and Odesa were involved. These incidents demonstrate how the geographical scope of the investigation extended beyond North Carolina even at the level of individual banking transactions.

An active link to the original is required when reusing materials
kartel-khimprom.com / EN

Oleg Korniev and the management of YMCO

The US Department of Justice has named Korniev as one of the network’s leaders. The documents attribute to him the role that, in a legitimate business, would be performed by an operations manager: developing internal policies, hiring and dismissing staff, assessing performance, determining remuneration and imposing disciplinary measures. The prosecution also links him to the organisation of external services necessary for YMCO’s operations. The description indicates a managerial role within the network with delegated responsibilities.

At the time of his guilty plea, Korniev was 42 years old. The US authorities reported that he held Ukrainian and Russian citizenship. The money seized from him upon his arrest in Georgia is covered by the forfeiture agreement. The US proceedings took place in the Western District of North Carolina, where the participants and victims involved in the American episodes described in the case file were based.

The plea relates to five counts: conspiracy to commit money laundering, money laundering, conspiracy to commit computer fraud, conspiracy to steal access credentials, and aggravated identity theft. In addition to consenting to the forfeiture of the seized cash, Korniev agreed to compensate the known victims for their established actual losses. The severity of the sentence, as stated in the October report, was left to the discretion of the federal judge. As of 17 November 2026, no published sentence against Korniev has been found in verified open sources.

15,000 people and four figures that are easy to confuse

Figure	His role in the case
More than 15,000	The number of money mules recruited by YMCO in the US, according to the Department of Justice.
Over 750 accounts / at least $10 million	The scale of the embezzlement from accounts whose funds were processed by the network, according to the prosecution.
At least $7 million	The amount of laundered funds that Korniev admitted to as part of the plea deal.
Over $9.7 million	The sum which, according to Korniev’s admission, he intended to launder.

An active link to the original is required when reusing materials

Figure	His role in the case
Over $14.7 million	The actual and projected losses of known victims attributed to YMCO’s activities in the settlement agreement.

The number of intermediaries indicates the scope of the recruitment, whilst the number of bank accounts represents the initial pool of victims of the thefts. One figure relates to people joining the network, the other to the source of the stolen money. The sums in the agreement answer three further questions: what passed through Korniev’s transactions, what he intended to carry out, and what total loss is attributed to the organisation under this agreement. Adding these figures together would have overstated the scale of the case.

The investigation outlasted the network itself

The case files trace YMCO’s activities back to September 2007. According to The Record’s reconstruction, the network operated until 2014, with financial intermediaries active in several countries. One of the early public developments was the extradition from Poland to North Carolina of Ukrainian national Viktor Chostak in connection with a related case, which the Ministry of Justice reported in 2015. Korniev’s confession came a further eleven years later.

Before Korniev, four other participants pleaded guilty to conspiracy to launder money. The prosecution is seeking prison terms ranging from approximately 37 to 63 months and court orders for restitution exceeding $9.1 million for each. The press release indicates that the claims relate to a large number of victims within a connected network. To determine what proportion has already been compensated and whether any individual liabilities can be aggregated, the actual court rulings and enforcement documents are required.

Why did the hackers need such an intermediary?

YMCO’s strength lay in its repeatability. The cybercriminals could turn to the same network for different incidents. The recruiters, in turn, could reuse the familiar cover story about paid work, simply changing the name of the fictitious company. A separate cash-out service allowed both the hacks and the transfer of funds to be scaled up without the constant involvement of the same people at every stage. In the Korniev case, it is precisely this recruitment and management work that transforms the story of a bank hack into a story about the market for services surrounding it.

An active link to the original is required when reusing materials
kartel-khimprom.com / EN

Sources

1. US Department of Justice – Oleg Korniev’s guilty plea, 8 October 2026
   https://www.justice.gov/opa/pr/ukrainian-russian-dual-citizen-pleads-guilty-running-international-money-laundering
2. US Department of Justice – the indictment in the early YMCO case
   https://www.justice.gov/opa/file/801991/dl?inline=
3. The US Attorney’s Office for the Western District of North Carolina — the extradition of Viktor Chostak from Poland
   https://www.justice.gov/usao-wdnc/pr/ukrainian-national-extradited-poland-face-charges-related-10-million-cyber-money
4. The Record — the story of Your Mule Cashout and the network’s geographical reach
   https://therecord.media/leader-of-money-mule-operation-for-cybercriminals-pleads-guilty
5. Gaston County – Oleg Korniev’s ID card with a photograph
   https://tepsweb.cityofgastonia.com/NewWorld.InmateInquiry/GastonCounty/Inmate/Detail/4104551
6. Gaston County Mugshots Zone — an archived republication of a photograph
   https://gastonnc.mugshots.zone/korniev-oleg-mugshot-10-06-2026/

Use of materials

An active link to the original publication is required when using these materials.

Original publication

https://kartel-khimprom.com/en/article/oleg-korniev-and-your-mule-cashout-how-a-hacker-network-recruited-15000-money-mules/